Remarks

[0001] Herein, the "Action" or "Office Action" refers to the Office Action dated October 26, 2006.

[0002] Applicant respectfully requests reconsideration and allowance of all pending claims of the application. Claims 1, 3, 8-16, 18-35, and 60-74 are presently pending. Claims withdrawn or canceled herein are 2, 4-7, 17, first claim 36, second claim 36, and claims 37-59. New claims added herein are claims 60-74. These new claims correspond to/are derived from the canceled claims as described on page 2 of this response, and these new claims have been added in order to correct the numbering confusion which resulted from the application being filed with two claims numbered claim 36.

Summary of Interview

[0003] Examiner Loving graciously talked with me—the undersigned attorney for the Applicant—on March 22, 2007. Applicant greatly appreciates the Examiners' willingness to talk. Such willingness is invaluable to both of us in our common goal of an expedited prosecution of this patent application.

[0004] In that discussion, I explained what I viewed as the differences between the cited art and the inventions described in the specification. We also discussed a possible amendment to claim 16. In response to a proposed amendment, Examiner Loving indicated that an

additional search may need to be performed. Applicant appreciates the Examiner's help in expediting the prosecution of this application.

Formal Request for an Interview

[0005] If the Office's reply to this communication is anything other than allowance of all pending claims, then Applicant formally requests an interview with the Examiner of this patent application. I encourage the Examiner to contact me—the undersigned attorney for the Applicant—to schedule a date and time for a telephone interview that is most convenient for both of us. Please email me at chrisf@leehayes.com. Should you contact me by email, please copy my assistant Carly Taylor (carly@leehayes.com) as well. While email works great for me, I welcome you to call either of us as well.

Claim Objections

[0006] Claim 8 and is objected to due to an informality (Office Action p.2). Appropriate corrections have been made herein.

[0007] There were two claims numbered 36 in the application as-filed. The examiner indicated that the second claim 36 (*i.e.*, the independent claim 36) will be treated as the parent claim in the office action. Appropriate correction has been made herein. More specifically, first claim 36, second claim 36, and claims 37-59 are canceled herein. New claims added herein are claims 60-74. These new claims correspond to the canceled claims as described on page 2 of this response, and the

new claims have been added in order to correct the numbering confusion which resulted from the application being filed with two claims numbered claim 36.

Substantive Claim Rejections

35 U.S.C. §101 Claim Rejections

[0008] Claims 29-35 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter (*Office Action* p.2). Appropriate correction has been made.

35 USC § 102 Claim Rejections

[0009] Claims 1-15, 29-36, and 45-49 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0172269 to Newcombe et al. (hereinafter, "Newcombe") (*Office Action* p. 3). Claims 2, 4-7, 36, and 45-49 are canceled herein, accordingly, the 102 rejection of these claims is moot.

[0010] Applicant respectfully traverses the remaining §102 rejections, and requests reconsideration and allowance in light of the comments and amendments contained herein. Accordingly, Applicant requests that the rejections be withdrawn and that the case be passed along to issuance.

[0011] **Independent Claim 1** recites a process for requesting authentication which can decrease problems associated with sham authentication requests, the process comprising:

> transmitting data from a hash digest formed using client-specific data together with second client specific data;
> receiving, in response to transmitting, an indication of acceptance when the data from the hash digest corresponds to a valid client authentication request; and
> prior to transmitting, computing the hash digest using the client name, client key and a function of time, and wherein transmitting includes transmitting a current time.

[0012] In order for Newcombe to anticipate this claim, Applicant submits that Newcombe must disclose each and every element and feature of the claim and that they must be arranged in the same manner as the claim. Applicant respectfully submits that Newcombe does not disclose all of the claimed elements and features of claim 1. For example, Newcombe does not show or disclose "prior to transmitting, computing the hash digest using the client name, client key and a function of time, and wherein transmitting includes transmitting a current time" as recited in claim 1.

[0013] Newcombe describes a method to help prevent an unauthorized user from accessing software via the Internet using a shared or stolen key or password (*Newcombe,* [0004]). To accomplish this goal, Newcombe describes that a client provides a request to an application authentication server, and the request includes a modified authenticator encrypted with a hashed salted password associated with a client

(*Newcombe,* [0025]). The modified authenticator binds a timestamp to the client by associating a remote IP address and a local IP address associated with the client to the timestamp, to minimize theft and reuse of an authenticator (*Newcombe,* [0025]). The authentication server is configured to receive the request from the client, and to use the client's local and remote IP addresses, and the user's salted password to extract the timestamp, and authenticate the user (*Newcombe,* [0025]). The authentication server examines the client's local and remote IP addresses to determine whether other unauthorized users are attempting to share the user's account, and authentication is based in part on the timestamp being within an acceptable time window (*Newcombe,* [0059]).

[0014] Newcombe does not show or disclose "prior to transmitting, computing the hash digest using the client name, client key and a function of time, and wherein transmitting includes transmitting a current time" as recited in claim 1. Instead, Newcombe describes interconnecting and hashing the local and remote IP addresses to obtain a value, and then binding the value with a timestamp to minimize theft and/or reuse of an authenticator.

[0015] Accordingly, claim 1 is allowable over Newcombe for at least these reasons, and Applicant respectfully requests that the §102 rejection be withdrawn.

[0016] **Claim 3** is allowable by virtue of its dependency upon claim 1. Additionally, claim 3 may be allowable over Newcombe for independent reasons.

[0017] **Independent Claim 8** recites a process for requesting authentication which can decrease problems associated with sham authentication requests, the process comprising:

> transmitting a hash digest formed from first client-specific data together with second client specific data;
> receiving, in response to transmitting, an indication of acceptance when the hash digest and second client-specific data correspond to a valid client authentication request; and
> receiving, in response to transmitting, a denial of authentication when the hash digest or the second client-specific data do not correspond to a valid client authentication request.

[0018] In order for Newcombe to anticipate this claim, Applicant submits that Newcombe must disclose each and every element and feature of the claim and that they must be arranged in the same manner as the claim. Applicant respectfully submits that Newcombe does not disclose all of the claimed elements and features of claim 8. For example, Newcombe does not show or disclose "receiving, in response to transmitting, a denial of authentication when the hash digest or the second client-specific data do not correspond to a valid client authentication request", as recited in claim 8.

[0019] Instead, as described previously, Newcombe describes obtaining local and remote IP addresses which are then combined with a timestamp. The local and remote IP addresses are used with user's hashed salted or randomly generated password to authenticate the user or client.

[0020] Accordingly, claim 8 is allowable over Newcombe for at least these reasons, and Applicant respectfully requests that the §102 rejection be withdrawn.

[0021] **Claims 9-15** are allowable by virtue of their dependency upon claim 8 (either directly or indirectly). Additionally, some or all of claims 9-15 may be allowable over Newcombe for independent reasons.

[0022] **Independent Claim 29** recites one or more computer-readable media having at least one tangible component and including instructions that, when executed by one or more processors, causes the one or more processors to:

> form an encrypted data string including first client-specific information;
>
> transmit a message including credentials formed using the encrypted data string together with second client-specific information; and
>
> receive a denial of authentication for system access, in response to the message, when the credentials are invalid; and
>
> store a portion of the client specific data in a cache memory along with an indication that the client specific data do not correspond to a valid client, the portion of the client specific data stored in the cache memory identifying a client name associated with the first client-specific information and associating the client name with a valid indication regardless of whether the first client-specific information included valid proof of knowledge for accessing privileged data.

[0023] In order for Newcombe to anticipate this claim, Applicant submits that Newcombe must disclose each and every element and feature of the claim and that they must be arranged in the same manner as the claim. Applicant respectfully submits that Newcombe does not disclose all of the claimed elements and features of claim 29. For example, Newcombe does not show or disclose "receive a denial of authentication for system access, in response to the message, when the credentials are invalid" and "store a portion of the client specific data in a cache memory along with an indication that the client specific data do not correspond to a

valid client, the portion of the client specific data stored in the cache memory identifying a client name associated with the first client-specific information and associating the client name with a valid indication regardless of whether the first client-specific information included valid proof of knowledge for accessing privileged data", as recited in claim 29.

[0024] Newcombe says nothing about storing a portion of the client specific data in a cache memory along with an indication that the client specific data do not correspond to a valid client, or that the portion of the client specific data stored in the cache memory identifying a client name is associated with the first client-specific information and that the client name is associated with a valid indication regardless of whether the first client-specific information included valid proof of knowledge for accessing privileged data, as recited in claim 29.

[0025] Accordingly, claim 29 is allowable over Newcombe for at least these reasons, and Applicant respectfully requests that the §102 rejection be withdrawn.

[0026] **Claims 30-35** are allowable by virtue of their dependency upon claim 29 (either directly or indirectly). Additionally, some or all of claims 30-35 may be allowable over Newcombe for independent reasons.

35 USC § 103 Claim Rejections

[0027] Claims 16-28, 36-44, and 50-59 are rejected under 35 U.S.C. §103(a) for obviousness over Newcombe in view of U.S. Patent No. 6,952,781 to Chang et al. (hereinafter, "Chang") (*Office Action* p. 10). Claims 17, 36-44, and 50-59 are canceled herein, accordingly, the 103 rejection of these claims is moot.

[0028] Applicant respectfully traverses each of the remaining §103 rejections, and requests reconsideration and allowance in light of the comments and amendments contained herein.

[0029] **Claim 16** recites a process for verification of a client authentication request by a server which can decrease problems associated with sham authentication requests, the process, comprising:

> receiving, in the server, a client authentication request including client-specific data;
>
> comparing the client specific data to data stored in a first cache memory coupled to the server to determine that the client specific data meet a first threshold of validity;
>
> when comparing determines that the client specific data meet the first threshold of validity, proceeding with the authentication process; and
>
> when comparing determines that the client specific data do not meet the first threshold of validity, then storing a portion of the client specific data in a second cache memory along with an indication that the client specific data do not correspond to a valid client, the portion of the client specific data stored in a second cache memory identifying a client name associated with the client authentication request and associating the client name with a valid indication regardless of whether the client specific data included valid proof of knowledge of privileged data, and then terminating the verification process.

[0030] Newcombe and/or Chang do not teach or suggest the combination of features recited in claim 16. For example, the Newcombe-Chang combination does not teach or suggest "comparing the client specific data to data stored in a first cache memory coupled to the server to determine that the client specific data meet a first threshold of validity" and "when comparing determines that the client specific data do not meet the first threshold of validity, then storing a portion of the client specific data in a second cache memory along with an indication that the client

specific data do not correspond to a valid client, the portion of the client specific data stored in a second cache memory identifying a client name associated with the client authentication request and associating the client name with a valid indication regardless of whether the client specific data included valid proof of knowledge of privileged data, and then terminating the verification process" as recited in claim 16.

[0031] The Office acknowledges that Newcombe fails to disclose a cache memory, and relies on Chang as disclosing a cache memory and curing the deficiencies of Newcombe (*Office Action* p.11; *Chang* Col.4 lns.17-24 and Col.6 lns.2-3).

[0032] Chang describes a mechanism for establishing a plurality of sessions between a client or user and a server based on single input of user identification information. The client sends a request for accessing the network resource, request includes identification information of the client. Depending upon the identification information, server determines whether to allow the access or not to the user and if allowed then connection should be established. If connection should be established then identification information will be stored in a cache memory. Due to caching operation multiple inputs for same identification information for access grant would be eliminated.

[0033] However, Chang fails to cure the deficiencies of Newcombe, as Chang does not teach or suggest that "when comparing determines that the client specific data do not meet the first threshold of validity, then

storing a portion of the client specific data in a second cache memory along with an indication that the client specific data do not correspond to a valid client, the portion of the client specific data stored in a second cache memory identifying a client name associated with the client authentication request and associating the client name with a valid indication regardless of whether the client specific data included valid proof of knowledge of privileged data, and then terminating the verification process" as recited in claim 16.

[0034] **Claims 18-23** are allowable over the Newcombe-Chang combination by virtue of their dependency upon claim 16. Claims 18-23 may also be allowable over the Newcombe-Chang combination for independent reasons.

New Claims Added

[0035] New claims 60-74 added herein. These new claims correspond to/are derived from the canceled claims as described on page 2 of this response, and these new claims have been added in order to correct the numbering confusion which resulted from the application being filed with two claims numbered claim 36. Applicant believes that claims 60-74 are allowable as presented for reasons similar to those described above in response to the 102 and 103 rejections. For convenience the added independent claims are reproduced and briefly discussed below.

[0036] **Independent Claim 61** (which corresponds to/is derived from second claim 36 (now canceled) which was rejected as obvious over the Newcombe-Chang combination) recites a computer system comprising:

> an authentication server; and
>
> a primary cache memory coupled to the authentication server, wherein the authentication server is configured to:
>
> receive a client authentication request including client-specific data;
>
> compare the client specific data to data stored in a first cache memory coupled to the server to determine that the client specific data meet a first threshold of validity;
>
> when comparing determines that the client specific data meet the first threshold of validity, proceed with authentication; and
>
> when comparing determines that the client specific data do not meet the first threshold of validity, terminate authentication and deny the authentication request;
>
> second compare the client specific data with data stored in the second cache memory to determine when the client specific data meet a second threshold of validity and when the client specific data correspond to an identity previously determined to be valid or invalid;
>
> when the client specific data meet the second threshold, transmit a request for verification to a database containing client-specific data; and
>
> when the client specific data correspond to an identity previously determined to be invalid, terminate the authentication request.

[0037] Newcombe and/or Chang do not teach or suggest the combination of features recited in claim 61. For example, the Newcombe-Chang combination does not teach or suggest "second compare the client specific data with data stored in the second cache memory to determine

when the client specific data meet a second threshold of validity and when the client specific data correspond to an identity previously determined to be valid or invalid; when the client specific data meet the second threshold, transmit a request for verification to a database containing client-specific data; and when the client specific data correspond to an identity previously determined to be invalid, terminate the authentication request" as recited in claim 61.

[0038] **Claims 62-68** are allowable over the Newcombe-Chang combination by virtue of their dependency upon claim 61. Claims 62-68 may also be allowable over the Newcombe-Chang combination for independent reasons.

[0039] **Independent Claim 69** (which corresponds to/is derived from claim 45 (now canceled) which was rejected as anticipated by Newcombe) recites a process for verification of a client authentication request by a server which can decrease problems associated with sham authentication requests, the process comprising:

> receiving, in the server, a client authentication request including client-specific data comprising a name or hash of the name along with a client key or some proof of knowledge which identifies the client key;
>
> comparing the client specific data to data stored in a first cache memory coupled to the server to determine that the client specific data meet a first threshold of validity, wherein the first cache memory stores names and keys of valid clients, and wherein the first cache memory uses the name or the hash of the name as a cashekey to access the first cache memory;
>
> when comparing determines that the client specific data meet the first threshold of validity since the name and the client key identified in the client authentication request corresponds to a valid entry in the first cache memory, proceeding with the authentication process; and
>
> when comparing determines that the client specific data do not meet the first threshold of validity since the name and the client key identified in the client authentication request does not correspond to a valid entry in the first cache memory, then storing the name and the client key in a second cache memory along validity/invalidity indicators, wherein the name stored in the second cache memory is associated with a valid indication regardless of whether the client key or the proof of knowledge for the client key matches data in an associated authentication database, and then terminating the verification process.

[0040] Applicant respectfully submits that Newcombe does not disclose all of the claimed elements and features of claim 69. For example, Newcombe does not show or disclose "comparing the client specific data to data stored in a first cache memory coupled to the server to determine that the client specific data meet a first threshold of validity, wherein the first cache memory stores names and keys of valid clients, and wherein the first cache memory uses the name or the hash of the name as a cashekey to access the first cache memory", as recited in claim 69.

[0041] Newcombe says nothing about a first cache memory which stores names and keys of valid clients, or that the first cache memory uses the name or the hash of the name as a cashekey to access the first cache memory, as recited in claim 69.

[0042] Further Newcombe does not show or disclose "when comparing determines that the client specific data do not meet the first threshold of validity since the name and the client key identified in the client authentication request does not correspond to a valid entry in the first cache memory, then storing the name and the client key in a second cache memory along validity/invalidity indicators, wherein the name stored in the second cache memory is associated with a valid indication regardless of whether the client key or the proof of knowledge for the client key matches data in an associated authentication database, and then terminating the verification process", as recited in claim 69.

[0043] Newcombe says nothing about a second cache memory, or about storing the name and the client key in the second cache memory along validity/invalidity indicators, as recited in claim 45. Newcombe also does not show or disclose that the name stored in the second cache memory is associated with a valid indication regardless of whether the client key or the proof of knowledge for the client key matches data in an associated authentication database, as recited in claim 69.

[0044] Accordingly, claim 69 is allowable over Newcombe for at least these reasons.

[0045] **Independent claim 70** (which corresponds to/is derived from second claim 50 (now canceled) which was rejected as obvious over the Newcombe-Chang combination) recites a process for authenticating a user which can decrease problems associated with sham authentication requests, the process, comprising:

> receiving an authentication request including first client specific data comprising at least one of a client name and proof of knowledge of a client key;
>
> computing a NameHash using the received client name and a random session key;
>
> using data corresponding to the NameHash as a cachekey to access first validity threshold data from a first cache memory;
>
> comparing the first validity threshold data to the first client specific data; and
>
> when comparing determines that the first client specific data do not meet the first threshold of validity, then storing a portion of the client specific data in a second cache memory along with an indication that the client specific data do not correspond to a valid client, the portion of the client specific data stored in a second cache memory identifying a client name associated with the client authentication request and associating the client name with a valid indication regardless of whether the client specific data included valid proof of knowledge of privileged data, and then terminating the verification process.

[0046] Newcombe and/or Chang do not teach or suggest the combination of features recited in claim 70. For example, the Newcombe-Chang combination does not teach or suggest "when comparing determines that the first client specific data do not meet the first threshold of validity, then storing a portion of the client specific data in a second

cache memory along with an indication that the client specific data do not correspond to a valid client, the portion of the client specific data stored in a second cache memory identifying a client name associated with the client authentication request and associating the client name with a valid indication regardless of whether the client specific data included valid proof of knowledge of privileged data, and then terminating the verification process" as recited in claim 70.

[0047] **Claims 71-74** are allowable over the Newcombe-Chang combination by virtue of their dependency upon claim 70. Claims 71-74 may also be allowable over the Newcombe-Chang combination for independent reasons.

Dependent Claims

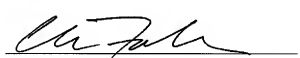
[0048] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0049] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Office is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Dated: 7-30-2007

By: 

Christen Fairborn
Reg. No. 55,164
(509) 324-9256 x249
chrisf@leehayes.com
www.leehayes.com